Approved ISMG Meeting Minutes

Date: May 26, 2011
Time: 1:00 pm
Location: Mitchell building, room 218

Attendees

Pat Boles, SITSD; Bill Hallinan, TRS; Larry Krause, COM; Cleo Anderson, DOR; Michael Sweeney, DOA; Chris Silvonen, DPHHS; Lynne Pizzini, SITSD; Kimberly Kessler, COR; Kristi Antosh, MDT; Rick Bush, DNRC; Byron Molyneaux, OPI; and Monica Abbott, SITSD.

Call to Order – Pat Boles

- Pat Boles called the May meeting to order and asked everyone for introductions.

Approval of Minutes – Pat Boles

- Pat asked for comments or changes to the April minutes. A correction is needed to the spelling of Rick Bush's name in the minutes. Pat will make the change.
  **** Action Item****
- Kristi Antosh offered a motion to approve the corrected minutes. Michael Sweeney seconded.
  - Motion passed unanimously.

Approval of Decision Brief Content – Rescind Internet Filtering (ENT-SEC-121) and Internet and Intranet Security (ENT-SEC-012) – Pat Boles

- Pat reported he tried to locate the decision brief 20100825 referenced in the background information section. He was able to locate a decision brief for 20100915, which is a decision brief on the legacy IT policy for remote access for contractors. This decision brief appears to have the criteria that were used to determine whether to retain, revise or rescind any policy being reviewed. Pat opened the discussion regarding rescinding the Legacy Internet Filtering and the Legacy Internet & Intranet Security policies.
- Rick Bush suggested changing the background from referencing the 20100825 brief to the 20100915 brief. Pat will take the criteria from the 20100915 brief and move it into the background information thereby eliminating any further references.
- Kristi Antosh mentioned the discussion in the past regarding the Internet & Intranet Security policy centered around its relationship to the network security that SITSD provides. This should be a service rather than a policy. She also indicated that since this policy [ENT-SEC-012] also references two other policies within it that are also being rescinded [ENT-SEC-021 and ENT-SEC-130] it is another indication that this is not a policy. The Internet Filtering Policy [ENT-SEC-121] discussion focused on the fact that this appears to be more of a procedure, and not a policy.
- Pat mentioned that SITSD offers internet connectivity services, is this Internet Filtering policy best viewed as an additional, value-add for those services? There is a default blocking certain sites to protect the aspects of the state's network, and that will continue, but exceptions are routinely granted for some of these sites based on business needs.

- Rick mentioned that these are service offerings, and not a policy. It is up to the agency of what filtering it wants.
- Lynne wants to see more documentation regarding rescinding the Internet Filtering Policy. She would like to see the procedures developed before rescinding. Kristi said that the decision brief recommendation #2 directs SITSD to communicate the procedure the Agencies would need to follow to modify the default configuration.
- The effective date of the policy being rescinded is July 1, 2012, which is in alignment with the implementation of the Information Security Programs Policy.
- Lynne wants the effective date added to the decision brief. Pat will add the date and criteria to the background.
- Lynne asked if we need the same added to the Internet & Intranet Security Policy. ** **Action Item****
- Rick Bush offered a motion to send the decision brief to SITSD executives. Bill Hallinan seconded the motion.
    - Motion passed unanimously.

Discuss NIST 800-39 Managing Information Security Risk – Organization, Mission, and Information System View – Published March 2011

- Pat spoke about managing risks using NIST 800-39 and the activities due by July 1, 2012.
- He referenced his presentation from the last meeting. The inputs from the organization lead into the activities, which is part of the Risk Frame process.
- Out of the process, the group will develop a Risk management Strategy document along with the organizational Policies, Standards and Guidance.
- Pat received a suggestion from Kristi to work as a group on an affinity diagram.
- The concept envisioned would review the activities outlined in NIST 800-39 and see if there is agreement among the group. Over the next few meetings, the group will build the risk management strategy document collectively. Agencies can then use this to develop their own risk management strategy by pulling out what is not pertinent to their respective agency.
- The group discussed the areas that are necessary for developing the document coming out of NIST.
- The first activity is to identify the assumptions. The second activity is to identify constraints.
- Pat located some risk management strategy documents from the United Kingdom.
- Pat will add the UK documents to the SharePoint site. He asked the group to review the documents over the next month. (These have been posted in the June meeting documents folder.)
- Rick asked if Pat made a request to Norex for Risk Management documents. Pat will check with Norex.
- Bill asked about how much of the Risk Management documents Pat referenced were focused on assumptions and constraints. Pat replied it was about a quarter of the 30-page document in the one UK example.
- The next activities are to identify Risk Tolerances followed by identifying the Priorities and Trade-offs.

- Pat will provide an outline to the affinity diagram activity for the next month. He asked how far the group wants to go at the next meeting.
- Bill asked if the outcome would be an affinity diagram exercise to cover as many of these activities as possible. The outputs of this exercise would be used to produce the collective Risk Management Strategy document.
- Rick mentioned additional contractual obligations reviewed within the agency. Kristi added that the overall point is having a document that indicates what the agency is addressing and why.
- Pat added the goal is to have an assessment after developing the Risk Management Strategy document. The document will guide agency's information risk management decisions. It will help identify EPP items for the next biennium, which comes out of the Risk Response phase of the risk management process.
- Some of decisions may be to change the business processes as a result of identifying threats and vulnerabilities, rather than implementing technical controls.
- Rick added the legal constraints section is important for agencies to comply with.
- Pat's presentation is available on the SharePoint site at: http://ent.sharepoint.mt.gov/groups/ism/Shared%20Documents/Meeting%20Documents/2011%20_03_March/Info_Risk_Mgmt_2011_03.pdf .

Updates – Pat Boles

- The security position in the Security Program Office will be a program manager not a bureau chief. The position is currently being reclassified.

Other Business or Concerns – ISMG

- Security training is going forward. MSISAC has asked how we would like to proceed with managing the security training. We can send a collective letter of intent and bill to a single agency (centralized) or each agency can send their own letter of intent. The centralized option will still allow agencies to see how users do on assessments. The centralized option would have a single pool of licenses for the state.
- Cost of license is $1.15 with $2 as the highest. Agencies can add users annually.
- There was verbal acclamation to go with the centralized option.
- Rick asked about getting CISSP training in Helena in the future. Lynne asked if he meant a boot camp for certification. Pat mentioned it is difficult to get the testing in Montana. The question for next month is how many would be interested.
- Kristi asked Lynne about the applications systems document availability that was mentioned in the previous meeting. Lynne sent a request to SABHRS, but has not heard back from SABHRS on releasing the document. She will follow up.
- Kristi asked about the two standards, 'Access Control' and 'Identification and Authentication'. Pat replied that they should go out for enterprise review next week.
- Bill was asked if the questions from the last meeting in regards to ASSERT had been addressed. Bill had not spoken to EPA yet. Bill will follow-up.

Adjourn – Pat Boles

- The meeting adjourned at 2:06 pm.